Sändlista sida 5-7

Ert tjänsteställe, handläggare
Signalskyddschefen

Ert datum

Er beteckning

Vårt tjänsteställe, handläggare
HKV MUST SÄKK SÄKT LS
Niklas Stråt, 08-788 70 68
niklas.straat@mil.se

Vårt föregående datum

Vår föregående beteckning

Författningskommentarer till FFS 2016:3 om signalskyddstjänsten

(1 bilaga)

Bakgrund

Under 2016 fastställde Försvarsmakten en ny och uppdaterad version av Försvarsmaktens föreskrifter (FFS) om signalskyddstjänsten med beteckningen FFS 2016:3. De tidigare föreskrifterna hade fastställts under 2005 och det förelåg ett behov av att uppdatera föreskrifterna bl.a. med anledning av olika tekniska, juridiska och organisatoriska förändringar inom sakområdet.

Regelverksöversyn

För närvarande pågår inom Försvarsmakten en regelverksöversyn i samband med införandet av en ny säkerhetsskyddslag, vilken förutses förändra tillsyns- och föreskriftsrätten inom säkerhetsskyddsområdet där även signalskyddstjänsten ingår. Regelverksöversynens främsta syfte är därför att revidera de centrala regelverk inom Försvarsmakten vilka har bäring på och berörs av den nya säkerhetsskyddslagen. Med centrala regelverk avses samtliga FFS och Försvarsmaktens Interna Bestämmelser (FIB) inom säkerhetsskyddsområdet, vilka därför kommer att revideras och uppdateras. Regelverksöversynsarbetet beräknas vara slutfört under 2018 och revideringen omfattar därför även FFS om signalskyddstjänsten som därför även den kommer att förändras i någon form.

Tillfällig ersättare till handbok

Normalt brukar även en reviderad handbok för signalskyddstjänsten ges ut något år efter det att en ny FFS om signalskyddstjänsten har fastställts. Med anledning av ovanstående regelverksöversyn, där bl.a. FFS om signalskyddstjänsten berörs och inom kort åter ska

revideras, hinner därför inte en reviderad handbok för signalskyddstjänsten ges ut. Denna skrivelse tjänar därför i ljuset av ovan anförda argument som en tillfällig ersättare till reviderad handbok för signalskyddstjänsten och innehåller för verksamheten relevanta författningskommentarer och förklarande text till Försvarsmaktens föreskrifter (FFS 2016:3) om signalskyddstjänsten.

Läsanvisningar

Författningskommentarerna och den förklarande texten återfinns inramad i bilaga 1 medan originalföreskriftstexten är kursiverad.

Vanligt förekommande frågor och allmän information

Med hänsyn till tidigare inkomna frågor och upplysningar som efterfrågats, vilka kan ge läsaren mer bakgrundsinformation och en bättre helhetsbild i läsandet av dessa föreskrifter, är det i sammanhanget värt att nämna följande allmänna företeelser och fakta rörande utarbetandet av signalskyddsföreskrifterna:

Varför ställer inte FFS om signalskydd t.ex. krav på användning av signalskydd för att även skydda sådan sekretess som inte rör rikets säkerhet?

Försvarsmaktens mandat inom signalskyddsområdet grundar sig främst på:

- 13§ säkerhetsskyddsförordning (SFS 1996:633) där det framgår att hemliga uppgifter endast får krypteras med ett kryptosystem som har godkänts av Försvarsmakten, samt

- 3 b, 33 §§ förordning (SFS 2007:1266) med instruktion för Försvarsmakten, enligt vilken Försvarsmakten dels ska leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information dels biträda Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet. Försvarsmakten får även meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner inom totalförsvaret.

Försvarsmakten ska med hänvisning till ovanstående låta utveckla kryptosystem som är dimensionerade för och säkra nog att kunna skydda Sveriges mest hemliga och känsliga information i form av uppgifter som omfattas av sekretess enligt 15 kap. 1, 2 §§ offentlighets- och sekretesslagen, OSL, (SFS 2009:400) och som rör rikets säkerhet[1].

Däremot har Försvarsmakten inte något mandat att föreskriva om kryptosystem för att skydda övriga sekretessbelagda uppgifter som inte rör rikets säkerhet enligt OSL. Exempel på sådan sekretess kan vara t.ex. sekretess till skydd för enskild i verksamhet som avser hälso- och sjukvård, så kallad patientsekretess, enligt 25 kap. 1 § OSL eller sekretess till skydd för intresset av att bevara djur- eller växtart enligt 20 kap. 1 § OSL.

[1] Definitionen av hemliga uppgifter enligt 4 § säkerhetsskyddsförordning (SFS 1996:633).

Varför omfattar inte FFS om signalskydd samtliga av Försvarsmakten utgivna aktiva kort, utan endast vissa?

I FFS om signalskydd regleras endast de aktiva korten NBK, TAK och TEID med anledning av att dessa aktiva kort får användas för att skydda olika typer av sekretessbelagd information.

- Nyckelbärarkortet, NBK, har som främsta syfte att användas som bärare av information i form av signalskyddsnycklar.

- Totalförsvarets Aktiva Kort, TAK, och Totalförsvarets Elektroniska ID-kort, TEID har som främsta syfte att på ett väldigt precist och kontrollerat sätt ge behöriga personer åtkomst till system och information samt på ett indirekt sätt skydda hemliga uppgifter i IT-system genom stark autentisering. TAK och TEID får även användas för att skydda sekretessbelagd information i form av signalskyddsnycklar.

NBK, TAK och TEID kan även innehålla annan sekretessbelagd information såsom certifikat och data. Övriga förekommande aktiva kort får inte (enligt respektive godkännandeskrivelse) innehålla någon sekretessbelagd information såsom nycklar, certifikat, data och/eller konfigurationer. Det avgörande är med andra ord inte vilken typ av information som återfinns på korten, utan det är i stället om de innehåller sekretess eller inte som är styrande.

Övriga förekommande aktiva kort såsom Databärarkort, DBK, eller Card for Encrypted Keys, CEK, regleras i manualer, handbok eller skrivelser, eftersom de inte ska hantera eller innehålla någon sekretessbelagd information.

Varför finns inte en lägre organisationsenhet än Högkvarteret omnämnd i FFS om signalskydd?

Enligt HKV LEDS JUR praxis får det aldrig i en FFS anges en organisationsenhet som är lägre än förband, skola eller center. Detta främst med tanke på att en FFS även kan reglera och styra andra myndigheter utanför Försvarsmakten, vilket är fallet med FFS om signalskydd då den styr statliga myndigheter som innehar någon form av signalskydd. En större organisatorisk detaljupplösning på försvarsmaktsnivå är i stället förbehållen en FIB inom samma sakområde där fler försvarsmaktsspecifika detaljer och organisationsenheter eller delar av dessa kan nämnas.

Måste jag som vanlig eller ny användare av signalskydd verkligen läsa igenom, detaljerat kunna samt förstå hela FFS om signalskydd?

FFS om signalskydd, samt alla andra FFS, är i första hand juridiska dokument som anpassats till juridiska mallar, juridisk nomenklatur och juridisk användning. En nybörjare inom signalskydd uppmuntras därför inte i första hand att endast läsa FFS utan i stället börja med den senaste utgåvan av signalskyddstjänstens handbok, eller som i detta fall, denna skrivelse. Skrivelsen innehåller dels alla paragrafer ur FFS om signalskydd med korta förklarande texter

till paragraferna som med ett mer vardagligt språk tydligare förklarar avsikten med varje enskild paragraf.

Beslut

Beslut i detta ärende har fattats av avdelningschef Pia Gruvö. I den slutliga handläggningen har dessutom deltagit sektionschef Peter Eidegren, Tina Brandt och som föredragande Niklas Stråat.

Gruvö, Pia

Chef Avdelningen för krypto och IT-säkerhet

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

Sändlista

Riksdagsförvaltningen
Sveriges riksbank
Regeringskansliet 4 ex (avsett för UD Säk, Fö, RK Säk och FA IT Krypto)
LG 3 ex (varav 1 ex vardera för MRM J2 och J6)
I 19 4 ex (varav 1 ex vardera för AJB, MRN J2 och J6)
K 3
P 4 3 ex (varav 1 ex vardera för MRV J2 och J6)
P 7 3 ex (varav 1 ex vardera för MRS J2 och J6)
A 9
Lv 6
Ing 2
LedR 3 ex (varav 1 ex vardera för TSS och MSK Ledsyst)
TrängR
1.ubflj
3.sjöstriflj
4.sjöstriflj
Amf 1
MarinB
F 7
F 17
F 21
Hkpflj
FMLOG 2 ex (varav 1 ex för Stab J2 Håkan Maltesson)
FMTIS 8 ex (avsett för J2, J5, J6, DriftE, SystE, SFE och SbE SbA)
SOG
MHS K
MHS H
MSS
SSS
LSS
HvSS
FMTS
SWEDEC
SkyddC
FM UndSäkC
FM HRC
FömedC
Försvarets materielverk 2 ex (varav 1 ex avsett för Kjell Albiin)
Försvarets radioanstalt 2 ex (varav 1 ex avsett för Sollefteå)
Försvarsunderrättelsedomstolen
Kustbevakningen
Myndigheten för samhällsskydd och beredskap 2 ex (1 ex avsett för Karlstad)
Rekryteringsmyndigheten
Statens inspektion för försvarsunderrättelseverksamhet

Totalförsvarets forskningsinstitut
Arbetsförmedlingen
Finansinspektionen
Riksgäldskontoret
Skatteverket
Statistiska centralbyrån
Tullverket
Brottsförebyggande Rådet
Domstolsverket
Ekobrottsmyndigheten
Kriminalvården 1 ex (avsett för Jakob Delden)
Migrationsverket
Polismyndigheten avsett för Nationella IT-avdelningen (Irene Nord) samt som orientering till Polisområdet i: Dalarna, Gotland, Gävleborg, Halland, Jämtland, Jönköping, Malmö, Norrbotten, ROE Toftanäs, Stockholm, Sydöstra Götaland Karlskrona, Södermanland, Uppsala, Värmland, Västerbotten, Västernorrland, Västmanland, Västra Götaland, Örebro och Östergötland
Rättsmedicinalverket
Säkerhetspolisen 6 ex (avsedda för Fredrik Ingemarsson och sektionerna)
Åklagarmyndigheten
Livsmedelsverket
Statens jordbruksverk
Statens veterinärmedicinska anstalt
Havs- och vattenmyndigheten
Strålsäkerhetsmyndigheten
Sveriges meteorologiska och hydrologiska institut (avsett för Norrköping)
Elsäkerhetsverket
Luftfartsverket (avsett för Norrköping)
Post och telestyrelsen
Sjöfartsverket
Statens energimyndighet
Svenska Kraftnät
Sveriges geologiska undersökning
Trafikverket
Transportstyrelsen 2 ex (avsedda för Torbjörn Sjöberg och Trafikregistret)
Folkhälsomyndigheten
Fortifikationsverket
Försäkringskassan
Lantmäteriet 2 ex (varav 1 ex vardera för Gävle och Geo-SE)
Läkemedelsverket
Länsstyrelsen i Blekinge, Dalarnas, Gotlands, Gävleborg, Halland, Jämtlands, Jönköpings, Kalmar, Kronobergs, Norrbottens, Skåne, Stockholms, Södermanlands, Uppsala, Värmlands, Västerbotten, Västernorrlands, Västmanlands, Västra Götalands (Göteborg + Vänersborg), Örebro och Östergötlands län
Socialstyrelsen

Statens fastighetsverk
Landstinget i Region Jämtland/Härjedalen, Stockholm och Västra Götalandsregionen
Försvarshögskolan
Folke Bernadotteakademin
Inspektionen för strategiska produkter
Sida
Forsmarks Kraftgrupp AB 742 03 Östhammar (avsett för Örjan Lindberg)
OKG AB 572 83 Oskarshamn (avsett för Anders Nilsson)
Ringhals AB 432 85 Väröbacka (avsett för Jan Karlsson)
Telia Sonera AB 405 35 Göteborg (avsett för Jonas Bergman)
Telia Sonera AB Box 336, 651 08 Karlstad (avsett för Jan Nilsson)
Teracom AB Box 30150, 104 25 Stockholm (avsett för Mikael Rappe)
Örebro läns flygplats AB 705 94 Örebro (avsett för Rolf Zandström)

Inom Högkvarteret
LEDS CIO
INSS J2
INSS J6
INSS SFL
ATS
MTS
FTS
PROD ARMÉ
PROD MARIN
PROD FLYG
PROD LEDUND 2 ex
MUST LEDK 2 ex (1 ex avsett för MUST signalskyddschef)
MUST SÄKK
MUST SÄKK SÄKU
MUST SÄKK SÄKS
MUST SÄKK SÄKT
MUST IHK
HKV AVD Säk (avsett för HKV signalskyddschef)

Bilaga 1

Försvarsmaktens föreskrifter om signalskyddstjänsten;

beslutade den 25 november 2016.

Försvarsmakten föreskriver med stöd av 33 § förordningen (2007:1266) med instruktion för Försvarsmakten följande.

1 kap. Allmänna bestämmelser

***1 §** Föreskrifterna i denna författning gäller för statliga myndigheter.*

Författningen gäller för statliga myndigheter, förutom regeringskansliet, riksdagen och dess myndigheter. Dock så tillämpas innehållet i författningen ändå i stort vid nyss nämnda myndigheter. Övriga som tilldelas signalskydd i någon form ska i ett avtal med en statlig myndighet förbinda sig att följa denna författning.

Definitioner

***2 §** I dessa föreskrifter avses med*

1. aktiva kort: kort som är utgivna av Högkvarteret och som får innehålla signalskyddsnycklar samt har försetts med någon av följande benämningar:

a) Totalförsvarets Aktiva Kort (TAK),

b) Totalförsvarets Elektroniska ID-kort (TEID), eller

c) Totalförsvarets Nyckelbärarkort (NBK),

Postadress Försvarsmakten 107 85 Stockholm
Besöksadress Lidingövägen 24
Telefon 08-788 75 00
Telefax 08-788 77 78
E-post, Internet exp-hkv@mil.se www.forsvarsmakten.se

2. enhet: en myndighets organisatoriska delar, såsom central ledning, regionala och lokala delar,

3. hemlig uppgift: uppgift som anges i 4 § 1 säkerhetsskyddsförordningen (1996:633),

4. Högkvarteret: Försvarsmaktens högkvarter,

5. internationell signalskyddsöverenskommelse: skriftlig överenskommelse som avser signalskydd mellan en svensk myndighet och en utländsk myndighet eller en mellanfolklig organisation,

En internationell signalskyddsöverenskommelse (även känd som signalskyddsavtal eller COMSEC-avtal) får endast förhandlas och ingås mellan en svensk myndighet och en utländsk myndighet eller internationell organisation under förutsättning att den svenska myndigheten har ett giltigt regeringsbemyndigande att förhandla och ingå en sådan signalskyddsöverenskommelse. Utländska företag är med dagens regelverk exkluderade från att kunna ingå internationella signalskyddsöverenskommelser direkt med svensk myndighet. Utländska företag anmodas då i stället, om det är oundgängligen nödvändigt, att söka stöd hos sitt lands *National Security Authority*-funktion, myndighet eller motsvarande. I dagsläget är det endast Försvarsmakten och FMV som innehar expertkompetens och bemyndigande från fall till fall inom signalskyddsområdet för att förhandla och ingå sådana överenskommelser.

6. kryptografiska funktioner: funktioner i ett system för

- att skydda information mot insyn och förvanskning, vid överföring och lagring med hjälp av kryptering,

- identifiering och autentisering,

- signering och verifiering av information, eller

- generering av signalskyddsnycklar,

7. nyckelansvarig myndighet: myndighet eller enhet som administrativt och operativt ansvarar för en viss nyckelserie,

Nyckelansvarig myndighet (NaM) kan vara en myndighet eller en enhet vid en myndighet. NaM:s främsta uppgift är att driftsätta myndighetsspecifika nyckelserier med begränsad spridning för att tillgodose myndighetens behov att skydda den egna verksamhetens information och behov av samverkan.

8. signalkontroll: kontroll av signalskyddet i telekommunikations- och IT-system i syfte att klarlägga dels riskerna för obehörig åtkomst eller störande eller förvanskning av data, dels att systemen används enligt gällande författning samt de säkerhetsmässiga krav som Högkvarteret meddelar,

9. signalskyddsincident:

- när en signalskyddsnyckel har eller kan antas ha röjts (nyckelincident),

- när signalskyddsmateriel saknas eller kan antas ha manipulerats eller utsatts för åverkan (materielincident), eller

- när ett aktivt kort saknas, kan antas ha manipulerats eller att obehörig kan antas ha haft tillgång till kortet (incident med aktivt kort),

10. signalskyddsmateriel:

- kryptoapparat,

- komponent, utrustning eller programvara som innehåller, eller avses innehålla, kryptografisk funktion och som ingår, eller avses ingå, i ett signalskyddssystem samt

- annan signalskyddsspecifik materiel eller programvara,

11. signalskyddsnycklar: nycklar som direkt eller indirekt är avsedda att skydda hemliga uppgifter,

Det tidigare begreppet "kryptonycklar" har nu ersatts av "signalskyddsnycklar". Signalskyddsnycklar ska ses som ett samlingsbegrepp för krypto-, system-, täck-, anrops-, lösen-, autentiserings-, frekvenshopps-, sessions-, privat- och packningsnycklar

12. signalskyddspersonal: personal som har signalskyddsbefattning som signalskyddschef, biträdande signalskyddschef, systemoperatör, nyckeladministratör eller kortadministratör,

13. signalskyddssystem:

- system med kryptografiska funktioner som är godkänt av Högkvarteret för skydd av uppgifter enligt bilaga 1 till denna författning, eller

- system för skydd mot obehörig insyn i och påverkan av telekommunikations- och IT-system som är godkänt av Högkvarteret,

14. signalskyddstjänst: verksamhet som syftar till att förhindra obehörig insyn i och påverkan av telekommunikations- och IT-system med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder,

15. telekommunikationssystem: system som innefattar tekniker för att överföra information mellan sändare och mottagare via ett trådlöst eller trådbundet medium.

"Telekommunikationssystem" ska i första hand tolkas som ett fjärrkommunikationssystem.

Signalskyddsgrader

3 § *I denna författning används begreppet signalskyddsgrader. Dessa indelas enligt följande: Top Secret (SG TS), Secret (SG S), Confidential (SG C), Restricted (SG R) samt Trafikskydd (SG TRF). Signalskyddsgradernas närmare betydelse anges i bilaga 1 till denna författning.*

En ny signalskyddsgrad har skapats i och med införandet av SG TRF. Denna signalskyddsgrad återfinns även i instruktionen/manualen Prov I Nycklar från 2010.

Användning av signalskyddssystem

4 § *Varje myndighet som har anskaffat eller tilldelats ett signalskyddssystem ska*

följa denna författning samt de säkerhetsmässiga krav som Högkvarteret meddelar avseende systemet och dess ingående delar.

En myndighet får endast konfigurera och använda ett signalskyddssystem på det sätt som framgår av Högkvarterets godkännande av systemet.

De säkerhetsmässiga krav som Högkvarteret meddelar kan vara i form av godkännanden, instruktioner, manualer eller övriga skrivelser som reglerar säkerheten kring ett signalskyddssystem.

Ledning och samordning av signalskyddstjänsten

5 § *Varje myndighet eller enhet som har ett signalskyddssystem ska ha en signalskyddschef. Signalskyddschefen har till uppgift att ansvara för ledning och samordning av signalskyddstjänsten.*

Om det finns särskilda skäl får en signalskyddschef vara signalskyddschef för andra enheter inom myndigheten, för en annan myndighet eller en eller flera av dess enheter efter överenskommelse mellan berörda myndigheter. En sådan överenskommelse ska dokumenteras.

Vid varje myndighet eller enhet som har ett signalskyddssystem utan att ha en signalskyddschef ska det finnas en biträdande signalskyddschef.

I de fall där en signalskyddschef agerar signalskyddschef för en annan myndighet eller annan enhet är det av stor vikt att detta bereds, beslutas samt dokumenteras på ett korrekt sätt inom de berörda myndigheterna eller enheterna då detta gäller en myndighets myndighetsutövning över en annan myndighet eller dess enheter, vilket kan vara känsligt samt juridiskt komplicerat i vissa fall.

6 § *Varje myndighet eller enhet som har aktiva kort ska ha en eller flera kortadministratörer.*

En myndighet eller enhet som endast nyttjar aktiva kort får i stället för en signalskyddschef ha en eller flera kortadministratörer. En kortadministratör ska ansvara för administration och redovisning av aktiva kort. Kortadministratörens

rutiner ska dokumenteras.

Dokumentationen kan med fördel göras i befintlig signalskyddsinstruktion, alternativt i ett särskilt framtaget dokument. Syftet är att dokumentationen ska klargöra och underlätta bedrivandet av en säker och kontinuerlig verksamhet.

7 § *Vid en nyckelansvarig myndighet ska det finnas en eller flera personer som har genomgått utbildning till nyckelansvarig. Nyckelansvarig ska ha det administrativa ansvaret för en eller flera nyckelserier vid myndigheten.*

Nyckelansvarig myndighets rutiner ska dokumenteras.

En Nyckelansvarig myndighet ska företrädas av en nyckelansvarig handläggare som tillsammans med en uppdragsgivare ska ansvara för driftsättning av nya nyckelserier, reglera användning och tilldelning, besluta om åtgärder i samband med incidenter samt avveckla densamma då den inte längre behövs i verksamheten. Dokumentationen kan med fördel göras i befintlig signalskyddsinstruktion, alternativt i ett särskilt framtaget dokument. Syftet är att dokumentationen ska klargöra och underlätta bedrivandet av en säker och kontinuerlig verksamhet.

8 § *En person får inneha flera signalskyddsbefattningar, roller eller ansvarsområden avseende signalskyddstjänsten vid en myndighet eller enhet som har ett signalskyddssystem.*

Denna paragraf har kommit till för att förtydliga att en person kan inneha flertalet signalskyddsbefattningar samtidigt. Dock så rekommenderas av redundansskäl en myndighet eller enhet aldrig att samtidigt ha färre än två personer som hanterar signalskyddet då problem med bemanning och säkerställandet av signalskyddet oftast kan uppstå vid t.ex. semester, sjukdom eller allvarliga olycksfall.

9 § *Varje myndighet och dess enheter som har ett signalskyddssystem ska i en handling (signalskyddsinstruktion) beskriva sin egen signalskyddsorganisation*

samt ange vilka åtgärder och uppgifter som krävs för att säkerställa signalskyddet, enligt bilaga 2 till denna författning. En sådan handling ska hållas uppdaterad.

Att ha en uppdaterad signalskyddsinstruktion är av största vikt för att kunna upprätthålla en hög säkerhetsnivå för de signalskyddssystem som används. De uppgifter som framgår av bilaga 2 är de grundläggande kraven som måste återfinnas i en signalskyddsinstruktion, övriga verksamhets- och säkerhetskrav som verksamheten ställer på signalskyddstjänsten ska även de dokumenteras i signalskyddsinstruktionen.

Krav på utbildning och behörighet

10 § *Endast den som med godkänt resultat har genomgått nödvändig utbildning i signalskydd får använda eller på annat sätt hantera signalskyddsmateriel, signalskyddsnycklar, aktiva kort eller inneha signalskyddsbefattning.*

Varje myndighet ska se till att personalen ges nödvändig utbildning.

Den som har genomgått utbildning med godkänt resultat ska få ett behörighetsbevis.

Det är av största vikt att de som använder signalskyddssystem också vet hur de ska använda systemen och hur de ska hantera incidenter med systemet. Behörighetsbevis skapar spårbarhet som bestyrker att utbildning skett med godkänt resultat.

11 § *Ett behörighetsbevis enligt 10 § får endast utfärdas av Försvarsmakten eller av den som av Försvarsmakten har godkänts som utbildare i signalskydd.*

Denna skrivning möjliggör att alla signalskyddslärare som utbildats av Försvarsmakten, samt andra signalskyddsbefattningar som får utbilda i signalskydd, kan signalskyddsutbilda användare och systemoperatörer även vid andra myndigheter och företag.

Kontroll av signalskyddstjänsten

Internkontroll

12 § *Varje myndighet eller enhet ska minst en gång per år, samt vid byte av signalskyddschef, genomföra kontroll av den egna signalskyddstjänsten. En kontroll ska avse myndighetens eller enhetens signalskyddsinstruktion och att gällande författning samt de säkerhetsmässiga kraven som Högkvarteret meddelar för signalskyddstjänsten följs. Det ska finnas en plan för hur denna kontroll ska genomföras.*

Myndigheten eller enheten ska föra protokoll över varje kontroll. Protokollen ska bevaras i minst 10 år och hållas samlade.

Protokollen från internkontrollerna ska för signalskyddstjänstens vidkommande bevaras i minst 10 år samt hållas samlade. Arkivlagen och andra regelverk som styr myndigheters hantering och arkivering av dessa allmänna handlingar (internkontrollprotokollen) gäller självklart i första hand. Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen. Företag som har signalskydd har t.ex. inte Arkivlagens krav på sig och för dessa företag är det mycket viktigt ur ett signalskyddshänseende att bl.a. internkontrollprotokollen sparas enligt den av författningen föreskrivna tiden.

Signalkontroll

13 § *En myndighet eller enhet ska se till att signalkontroll genomförs i den omfattning som behövs för att konstatera om signalskyddet är tillräckligt.*

Har en myndighet eller enhet genomfört signalkontroll ska fel eller brister som upptäckts vid kontrollen och som inte är av ringa betydelse anmälas till Högkvarteret.

Varje myndighet eller enhet som har fått del av resultatet av en signalkontroll ska utan dröjsmål vidta de åtgärder som krävs för att säkerställa signalskyddet.

Att fel eller brister som inte är av ringa betydelse ska anmälas till Högkvarteret ska läsas som att uppgifter som har placerats i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre och vilka kan ha röjts p.g.a. fel eller brister i signalskyddet, ska anmälas till Högkvarteret.

2 kap. Signalskyddsnycklar

1 § *Signalskyddsnycklar som är märkta med SG TS, SG S eller SG C får inte läsas in, förvaras, produceras eller användas i en utrustning som mellanlagrar signalskyddsnycklarna i klartext på permanent lagringsmedium.*

Med "en utrustning som mellanlagrar signalskyddsnycklarna i klartext på permanent lagringsmedium" menas t.ex. en kopiator med hårddisk, en scanner, ett USB-minne etc. Det har hänt att användare har kopierat signalskyddsnycklar på kopiator med hårddisk ovetande om att signalskyddsnycklarna då sparats på kopiatorns hårddisk, vilken inte är en säker lagringsplats samt att den är utanför användarens kontroll med tanke på servicepersonal, nätverksanslutning m.m.

Produktion

2 § *Signalskyddsnycklar får endast produceras i utrustning samt med programvara och metoder som har godkänts av Högkvarteret.*

Produktion av signalskyddsnycklar får endast ske på sådant sätt att obehöriga inte får insyn i verksamheten.

Sådan produktion sker oftast centralt på Högkvarteret och ibland ute i verksamheten med produktionssystemet Lokal nyckelproduktion (LNP). Vissa signalskyddssystem kan även producera egna nycklar, t.ex. PGBI och MGKI.

3 § *Vid produktion av signalskyddsnycklar, som inte enbart existerar i elektronisk form, ska varje enskilt exemplar märkas med uppgift om vilket signalskyddssystem som nyckeln är avsedd för, nyckelserie, giltighetstid,*

lottningsnummer och signalskyddsgrad samt i förekommande fall kryptobeteckning.

Signalskyddsnycklar ska även förses med sekretessmarkering och exemplarnummer.

Produktion av signalskyddsnycklar ska dokumenteras. Av dokumentationen ska framgå vilket signalskyddssystem som nyckeln är avsedd för, nyckelserie, signalskyddsgrad, nyckelns giltighetstid, dess lottningsnummer och exemplarnummer.

Dokumentationen ska bevaras i minst 10 år efter det att respektive nyckel har upphört att gälla.

Märkning och dokumentation av producerade signalskyddsnycklar är viktigt ur säkerhetssynpunkt och måste ske för att tilltron till systemet ska hållas hög.
Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

Avskrift eller kopiering

4 § *En avskrift eller kopia av en signalskyddsnyckel får endast göras efter tillstånd av nyckelansvarig myndighet. Ett sådant tillstånd ska dokumenteras.*

En avskrift eller kopia av en signalskyddsnyckel ska märkas med samma information som anges i 3 § första och andra styckena. En sådan avskrift eller kopia ska dokumenteras och dokumentationen ska innehålla samma uppgifter som anges i 3 § tredje stycket.

Avskrift eller kopiering av signalskyddsnycklar ska endast undantagsvis göras och då mycket restriktivt. Risken med kopiering är att den som ska kopiera signalskyddsnyckeln använder fel sorts utrustning, vilket kan innebära att nyckeln exponeras otillbörligen och då kan anses vara röjd (se även kommentaren ovan gällande 2 kap 1 §).

Förpackning, distribution och mottagning

5 § *Varje myndighet ska se till att nödvändiga skyddsåtgärder vidtas vid distribution av signalskyddsnycklar.*

Signalskyddsnycklar som gäller och signalskyddsnycklar som har upphört att gälla får inte distribueras per post. Signalskyddsnycklar som inte har börjat gälla får distribueras per post.

Distribution av signalskyddsnycklar via telekommunikation får inte ske utan tillstånd av nyckelansvarig myndighet.

Signalskyddsnycklar som är gällande, giltiga eller har tagits i bruk samt signalskyddsnycklar som har slutat att gälla, får inte skickas med post av den enkla anledningen att de är eller har varit i skarp drift och därmed är de som mest sårbara om någon obehörig skulle komma åt dem i transit. Signalskyddsnycklar som ännu inte har börjat gälla och där utgivaren vet att samtliga försändelser kommit fram till slutmottagaren genom mottagningsbevissystemet, får anses vara framgångsrikt och säkert levererade.

Distribution av signalskyddsnycklar via telekommunikation är en ur kryptologisk synpunkt dålig lösning då det skulle räcka för en motståndare att få tag på en enda nyckel för att sedan med hjälp av den få tag på alla andra som i sin tur krypteras med den.

6 § *Signalskyddsnycklar ska distribueras i ett förseglat emballage. Emballaget ska vara så beskaffat att det är omöjligt att ta del av innehållet utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget.*

Det förseglade emballaget ska innehålla ett förseglat innerkuvert, som ska vara försett med påskrift att det innehåller signalskyddsnycklar och att det ska överlämnas obrutet till den som är signalskyddschef eller till den som myndigheten eller enheten har bestämt.

Emballage kan vara kuvert förseglat med säkerhetstejp eller säkerhetspåse. Innerkuvertet syftar till att inte exponera nycklarna i onödan för exempelvis expeditionspersonal som tar emot försändelsen.

7 § *Distribution av signalskyddsnycklar ska dokumenteras.*

Dokumentationen kan göras i ett av myndigheten utpekat system eller i ett separat dokument.

8 § *När signalskyddsnycklar distribueras ska ett mottagningsbevis och en följesedel bifogas i försändelsen. Av följesedeln ska framgå vilket signalskyddssystem som nyckeln är avsedd för, nyckelserie, nyckelns giltighetstid, dess lottningsnummer och exemplarnummer samt till vilken myndighet eller enhet respektive nyckel har distribuerats.*

Följesedeln för signalskyddsnycklar som är märkta med SG TS ska registreras och bevaras i minst 25 år av avsändare och mottagare efter det att respektive nyckel har upphört att gälla.

Följesedeln för signalskyddsnycklar märkta med SG S, SG C, SG R eller SG TRF ska registreras och bevaras av avsändare och mottagare i minst 10 år efter det att respektive nyckel har upphört att gälla.

Det är viktigt att mottagningsbeviset och följesedeln bipackas innerkuvertet där signalskyddsnycklarna finns. Detta för att det är signalskyddschefen eller annan utsedd person som tar emot nycklarna som ska kontrollera att alla nycklar finns med enligt följesedeln samt därefter snarast återsända mottagningsbeviset. Försvarsmakten är numera en registratormyndighet vilket innebär att där en handling (exempelvis en följesedel) upprättas där ska handlingen också registreras. Handlingar som skickas och tas emot inom Försvarsmakten behöver mottagande enhet inte registrera då handlingen redan är registrerad av upprättande enhet. Är däremot handlingen att betrakta som inkommen från annan myndighet eller verksamhet ska den registreras där den inkom.

Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

9 § *Vid mottagning av en försändelse med signalskyddsnycklar ska innehållet i försändelsen skyndsamt kontrolleras mot bifogad följesedel. Mottagningsbeviset ska därefter snarast undertecknas och återsändas till avsändaren.*

Överensstämmer inte innehållet i försändelsen mot bifogad följesedel ska avsändaren omedelbart underrättas.

Det är för signalskyddstjänsten viktigt att innehållet kontrollräknas skyndsamt så att eventuella misstag kan rättas till.

Delgivning

10 § *Signalskyddsnycklar får endast delges den som bedöms pålitlig ur säkerhetssynpunkt, har tillräckliga kunskaper om säkerhetsskydd, behöver nycklarna för sitt arbete i den verksamhet där de ska hanteras samt har fått nödvändig utbildning i signalskydd och hantering av signalskyddsnycklar.*

Signalskyddspersonal som har tillgång till signalskyddsnycklar ska förtecknas. Övriga som delges signalskyddsnycklar ska kvittera mottagandet.

Förteckningar och kvittenser för signalskyddsnycklar märkta med SG TS ska bevaras i minst 25 år.

Förteckningar och kvittenser för signalskyddsnycklar märkta med SG S, SG C, SG R eller SG TRF ska bevaras i minst 10 år.

Kravet på bevarandet överensstämmer med de krav som finns för hemliga handlingar enligt FFS 2015:2 Säkerhetsskydd samt PMFS 2015:3 Säkerhetsskydd. Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

Hantering och förvaring

11 § *Signalskyddsnycklar ska hanteras så att någon obehörig inte kan ta del av nyckeln.*

Verksamheten behöver göra en analys på hur signalskyddsnycklar hanteras och hur obehörig insyn kan förhindras. Det kan exempelvis vara att dörrar till utrymmen där signalskyddsnycklar hanteras förses med inpasseringskontroll och att gardiner dras för fönster vid hantering av nycklar men också att nycklar inte hanteras i en reception där obehörig personal normalt uppehåller sig och att säkerhetsskåp som innehåller signalskyddsnycklar inte placeras ute i korridorer. Detta gäller särskilt signalskyddsnycklar i pappersform vilka är i klartext, s.k. röda nycklar, och därför är mycket känsliga för exponering.

12 § *Signalskyddsnycklar som är märkta med SG TS, SG S eller SG C ska förvaras i ett utrymme som uppfyller lägst kraven för värdeskåp enligt Svensk Standard (SS) 3150 med lägre än 100 skyddsvärdespoäng, säkerhetsskåp enligt Svensk Standard (SS) 3492 eller Svensk Standard (SS-EN) 1143-1 grade 0-III eller stå under ständig uppsikt i syfte att uppnå erforderligt skydd.*

Signalskyddsnycklar som är märkta med SG TS ska hållas åtskilda från signalskyddsnycklar som är märkta med en annan signalskyddsgrad.

Signalskyddsnycklar som är märkta med SG R eller SG TRF ska förvaras inlåsta eller förvaras i en lokal som endast den som är behörig att ta del av nycklarna har tillträde till eller stå under ständig uppsikt i syfte att uppnå erforderligt skydd.

Den nu utgångna licensen till standarden SS 3492 har fortfarande ett tillräckligt säkerhetsskydd, förvaras signalskyddsnycklar enligt denna standard uppfylls fortfarande kravet trots att licensen gått ut. Att SG TS-nycklar ska hållas åtskilda innebär att nycklarna ska förvaras fysiskt separerade från andra signalskyddsnycklar i exempelvis en för ändamålet avsedd

pärm, låda eller innerfack inne i det godkända förvaringsutrymmet. Nyckelansvarig myndighet kan komma med ytterligare krav på förvaring i dennes driftsättningsskrivelse.

13 § *Varje myndighet eller enhet får först efter överenskommelse med nyckelansvarig myndighet fatta beslut som avviker från 12 § första stycket, under förutsättning att tillräcklig säkerhetsskyddsnivå kan upprätthållas. Ett sådant beslut ska dokumenteras.*

Detta överensstämmer med Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2015:2) och kan med fördel läsas som vägledning för hur en motsvarande skyddsnivå kan upprätthållas.

Utförsel utanför svenskt territorium

14 § *För att få föra ut eller på annat sätt göra signalskyddsnycklar tillgängliga utanför svenskt territorium krävs*

1. *att signalskyddsnycklarna är avsedda att användas för internationellt bruk, och*
2. *att nyckelansvarig myndighet, först efter överenskommelse med Högkvarteret, har beslutat att utförsel får ske samt hur nycklarna ska hanteras.*

Signalskyddsnycklar som endast är avsedda att användas för nationellt bruk inom svenskt territorium får inte medföras utanför territoriet utan särskilt godkännande av Högkvarteret.

Nycklar som är avsedda för internationellt bruk ska vara märkta med tilläggsbeteckningen INT i serienamnet (se Prov I Nycklar).
Nyckelansvarig myndighet (NaM) är den verksamhet som driftsatt en nyckelserie för ett särskilt ändamål och det är av stor vikt att NaM har beslutat om utförsel först efter samråd med avdelningen för krypto och IT-säkerhet (SÄKT) inom den militära underrättelse och säkerhetstjänsten (MUST) vid

Högkvarteret. Detta samråd kan gälla över tid eller för en särskild verksamhet och behöver inte nödvändigtvis ske vid varje utförseltillfälle.
Vid Försvarsmakten finns ett särskilt godkännande i en intern bestämmelse, 29 § FIB 2008:3, att fartyg och luftfartyg som kortvarigt lämnar svenskt territorium för övningsverksamhet eller en nationell insats får föra ut de kryptonycklar som oundgängligen behövs för att kunna genomföra övningen eller insatsen. Kryptonycklarna ska om möjligt tas ur särskilda kryptonyckelserier.

Inventering

15 § *Inventering av signalskyddsnycklar ska göras vid ett långvarigt byte av signalskyddspersonal som ansvarar för signalskyddsnycklar.*

Utöver vad som föreskrivs i första stycket ska odaterade signalskyddsnycklar inventeras varje år.

Signalskyddsnycklar som är märkta med SG TS ska inventeras av signalskyddschefen eller biträdande signalskyddschef samt ytterligare en signalskyddsutbildad person.

Signalskyddsnycklar med annan signalskyddsgrad ska inventeras av signalskyddschefen eller en av myndigheten utsedd signalskyddsutbildad person.

Med långvarigt byte menas exempelvis 6 månaders tjänstledighet eller utbildning, alltså längre än en normal semester på fyra veckor.
Normalt behöver inte signalskyddsnycklar inventeras då de ska förstöras när de upphört att gälla eller inte längre behövs för tjänsten, undantaget är odaterade nycklar som exempelvis kan vara beredskapsnycklar som först tas i drift på order eller andra lottningsnummernycklar som fördelats ut och förvaras ute i verksamheten lång tid innan användning.

16 § *Inventering av signalskyddsnycklar ska dokumenteras.*

Dokumentationen avseende signalskyddsnycklar som är märkta SG TS ska bevaras i minst 25 år.

Dokumentationen avseende signalskyddsnycklar med en annan signalskyddsgrad ska bevaras i minst10 år.

Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen

Rutinmässig förstöring och radering

17 § *Varje signalskyddsnyckel ska snarast förstöras och, avseende nyckel som lagras elektroniskt, raderas när den har upphört att gälla eller när den inte längre behövs för tjänsten.*

Förstöring av signalskyddsnycklar ska utföras av en signalskyddsutbildad person.

Det är av största vikt att de som använder signalskyddssystem också vet hur och när de ska förstöra signalskyddsnycklar på ett korrekt sätt. Underrättelsevärdet för en signalskyddsnyckel är som högst när nyckeln har använts eller används vilket ställer höga krav på att alla exemplar av signalskyddsnycklarna förstörs när de har upphört att gälla eller inte längre behövs för tjänsten.

18 § *Förstöring av signalskyddsnycklar ska dokumenteras.*

Dokumentationen avseende signalskyddsnycklar som är märkta SG TS ska bevaras i minst 25 år.

Dokumentationen avseende signalskyddsnycklar med en annan signalskyddsgrad ska bevaras i minst 10 år.

Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen

19 § *Signalskyddsnycklar ska förstöras på ett sådant sätt att det är omöjligt att återskapa och ta del av hela, eller delar av, signalskyddsnyckeln.*

Det innebär att en spånstorlek på 2 x 2 mm storlek eller mindre förordas vid förstöring av kryptonycklar.

I övrigt så kan signalskyddsnycklar anses vara förstörda om restprodukten har en spånlängd av 15 mm i längd och 1,2 mm i bredd eller mindre för att säkerställa att nyckeln inte ska kunna återskapas efter destruktion. Med denna typ av destruktion krävs det att kryptonyckel av streckkodstyp matas in på rätt sätt i destruktören så att inte flera streckkodsstreck finns på varje sådant spån.
Signalskyddsnycklar kan även förstöras genom eldning, viktigt att tänka på då är att sotflagor och restprodukter förbränns tills dess att det inte finns några restprodukter kvar än omrörd aska.

Åtgärder vid nyckelincident

20 § *Den som har förlorat en signalskyddsnyckel eller misstänker eller på annat sätt har fått uppgift om att en signalskyddsnyckel kan vara röjd, ska omedelbart anmäla detta till nyckelansvarig myndighet och myndighetens eller enhetens signalskyddschef samt säkerhetsskyddschef.*

Nyckelansvarig myndighet ska

1. avgöra om signalskyddsnyckeln kan ha röjts och meddela berörda enheter om vilka åtgärder som ska vidtas för att återställa signalskyddet, och

2. orientera den enhet i Högkvarteret som har till uppgift att leda och samordna signalskyddstjänsten inom totalförsvaret om vidtagna åtgärder och om anledningen till dessa.

Nyckelansvarig myndighet (NaM) har att fatta beslut om vilka åtgärder som ska vidtas vid en incidentanmälan. En första åtgärd bör vara att snabbt fatta beslut och informera alla användare av nyckelserien om nyckeln ska tas ur drift eller inte, samt hur signalskyddet ska upprättas igen. Därefter kan fortsatt efterforskning kring omständigheterna slutföras och ytterligare beslut kan fattas med efterföljande information till användarna om nyckeln är att betrakta som röjd, misstänkt röjd eller inte röjd.
Inom Försvarsmakten är en incident med signalskyddsnycklar att betrakta som en säkerhetsincident och ska även rapporteras som en säkerhetshändelse till

regional stab eller Högkvarter. För övriga myndigheter gäller respektive myndighets säkerhetsbestämmelser.

3 kap. Signalskyddsmateriel

Utveckling och upphandling

1 § *En myndighet som utvecklar eller tillverkar, eller låter utveckla eller tillverka materiel som avses bli signalskyddsmateriel ska se till att*

1. det som grund för kravställning inför varje materielutveckling eller tillverkning görs en säkerhetsanalys och en säkerhetsplan som tar hänsyn till signalskyddets särskilda krav,

2. utveckling eller tillverkning av kryptoalgoritmer och övriga säkerhetsfunktioner i signalskyddsmateriel sker i IT-system som är godkända ur säkerhetssynpunkt (ackrediterade) först efter överenskommelse med Högkvarteret,

3. en hemlig kryptoalgoritm som är framtagen för ett visst system inte används i ett annat system utan skriftligt godkännande av Högkvarteret, och

4. sådan signalskyddsmateriel, signalskyddssystem eller del av signalskyddssystem, inte, utan godkännande av Högkvarteret, säljs eller överlämnas till någon annan än den myndighet som materielen är avsedd för.

Säkerhetsanalys och säkerhetsplan enligt första stycket 1 får fastställas först efter överenskommelse med Högkvarteret.

Denna paragraf riktar sig främst till Försvarsmaktens produktionsdelar som i sitt arbete utvecklar eller tillverkar, eller låter utveckla eller tillverka materiel som avses bli signalskyddsmateriel.

Det är viktigt att det finns en god dialog mellan FMV och Försvarsmakten för att bibehålla en hög säkerhetsnivå genom hela utvecklings- och tillverkningsprocessen.

2 § *En myndighet som upphandlar materiel som avses bli signalskyddsmateriel, eller programvara för sådan materiel, ska se till att leverantören förbinder sig att hantera materielen på ett sätt som säkerställer att den är säker att använda för avsett syfte.*

Denna paragraf riktar sig främst till FMV som i sitt arbete upphandlar utveckling och tillverkning av signalskyddsmateriel.

Försegling och märkning

3 § *Signalskyddsmateriel, utom signalskyddsspecifik programvara, ska vara förseglad, med plombering eller lås, så att den som hanterar materielen kan upptäcka om någon har försökt manipulera den.*

Försegling och lås är ett manipulationsskydd som är väsentligt för säkerheten kring signalskyddssystemen. För att uppnå hög säkerhet krävs att användaren kontrollerar försegling och lås vid användandet av signalskyddssystemet.

4 § *Signalskyddsmateriel som innehåller kryptografiska funktioner, godkända för skydd av uppgifter enligt bilaga 1 till denna författning, ska vara märkt med beteckningen SWE CCI (Swedish Controlled Cryptographic Item).*

Signalskyddsmateriel som inte innehåller kryptografiska funktioner ska vara märkt med beteckningen SWE CI (Swedish Controlled Item).

SWE CCI och SWE CI är internationellt erkända märkningar som tydliggör att det finns ett särskilt regelverk kring förvaring, hantering och användning av signalskyddssystem. SWE CCI-märkt signalskyddsmateriel innehåller i normalfallet en kryptomodul, t.ex. kryptoapparat 491 i signalskyddssystem MGM (kryptofaxsystemet). SWE CI-märkt signalskyddsmateriel kallas även signalskyddsnära materiel och innehåller ingen kryptomodul men är väsentlig för att signalskyddssystemet ska fungera, t.ex. själva faxen i signalskyddssystem MGM (kryptofaxsystemet).

Hantering

5 § *Signalskyddsmateriel får endast hanteras av den som har tillräckliga kunskaper om säkerhetsskydd, behöver signalskyddsmaterielen för sitt arbete i den verksamhet där materielen ska hanteras samt med godkänt resultat har fått nödvändig utbildning i signalskydd.*

Då signalskyddsmateriel är att betrakta som skyddsvärd, och då främst med tanke på dess tänkta användningsområde, så ställer vi krav på dem som ska hantera den. För att uppnå en hög säkerhet krävs utbildning innan signalskyddssystemen får användas. Normalt utbildar Totalförsvarets signalskyddsskola signalskyddschefer och signalskyddslärare. Myndigheten med dess verksamheter har sedan normalt till uppgift att bland annat utbilda användare, systemoperatörer, förrådspersonal och nyckeladministratörer.

Förpackning och försändning

6 § *Vid försändning av signalskyddsmateriel ska emballaget vara så beskaffat att det är omöjligt att få information om materielen utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget.*

Vid mottagning av en försändelse med signalskyddsmateriel ska snarast

- emballagets försegling kontrolleras, samt

- innehållet i försändelsen kontrolleras mot bifogad följesedel eller kvitto.

Vid bruten försegling eller då innehållet i försändelsen inte överensstämmer mot bifogad följesedel eller kvitto ska avsändaren snarast underrättas.

Signalskyddsmateriel är att betrakta som skyddsvärd främst med tanke på dess tänkta användningsområde men även p.g.a. att utrustningen är dyr och finns i begränsad mängd. Med anledning av ovanstående ska signalskyddsmateriel försändas enligt myndighetens krav för skyddsvärd materiel.

Emballage kan vara kartong förseglat med säkerhetstejp eller säkerhetspåse. Det kan också vara transportbehållare 601 eller 602 där låsnycklar till

transportbehållare samt eventuella låsnycklar till signalskyddsutrustning sänds separat med ”Posten värde” eller motsvarande.
Det är för signalskyddstjänsten viktigt att innehållet kontrolleras skyndsamt så att eventuella misstag kan rättas till.
Försvarsmakten är numera en registratormyndighet vilket innebär att där en handling upprättas där ska handlingen också registreras. Skickas och mottas handlingar inom Försvarsmakten behöver mottagande enhet inte registrera handlingen då den redan är registrerad av upprättande enheten. Är handlingen att betrakta som inkommen från annan myndighet eller verksamhet ska den registreras där den inkom.

Kvittering

7 § *När signalskyddsmateriel lämnas ut ska signalskyddschefen eller den som lämnar ut materielen se till att signalskyddsmaterielen kvitteras av behörig användare eller signalskyddspersonal. Kvittensen ska bevaras under den tid som materielen är utlämnad.*

Signalskyddsmateriel är att betrakta som skyddsvärd främst med tanke på dess tänkta användningsområde men även p.g.a. att utrustningen är dyr, finns i begränsad mängd och därför behöver den kvitteras. Kvittering är också ett sätt att säkerställa personligt ansvar och detaljerad spårbarhet och uppföljning av signalskyddsmaterielen.
Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

Placering och förvaring

8 § *En myndighet eller enhet ska vidta säkerhetsskyddsåtgärder i syfte att förhindra manipulation och tillgrepp av signalskyddsmateriel. Åtgärderna ska dokumenteras.*

Signalskyddsmateriel med inlästa signalskyddsnycklar ska hanteras och förvaras på samma sätt som föreskrivs om signalskyddsnycklar i 2 kap. 11–13 §§.

Säkerhetsskyddsåtgärderna kan med fördel dokumenteras i den ordinarie signalskyddsinstruktionen och kan innehålla krav på att exempelvis utrymmen såsom kontorsrum och förråd där signalskyddsmateriel utan inlästa signalskyddsnycklar förvaras eller används ska hållas låsta om ingen behörig personal finns i utrymmet.

Signalskyddsmateriel med inlästa signalskyddsnycklar övertar nycklarnas klassning när de är inlästa i signalskyddsmaterielen, vilket innebär att signalskyddsmaterielen då måste stå under ständig uppsikt, att den hålls under kontroll eller låsas in i ett säkerhetsskåp när det gäller signalskyddsnycklar märkta med SG C, SG S och SG TS. För signalskyddsnycklar märkta med SG R och SG TRF gäller ständig uppsikt, att den hålls under kontroll alternativt inlåsta eller förvarade i en lokal som endast den som är behörig att ta del av nycklarna har tillträde till.

Utförsel av signalskyddsmateriel utanför svenskt territorium

9 § *För att få föra ut signalskyddsmateriel utanför svenskt territorium krävs godkännande av Högkvarteret eller den enhet som Högkvarteret bestämmer.*

Avdelningen för krypto och IT-säkerhet (SÄKT) inom den militära underrättelse och säkerhetstjänsten (MUST) vid Högkvarteret kan efter överenskommelse godkänna utförsel över tiden eller för en särskild verksamhet, s.k. stående utförseltillstånd.

Redovisning och inventering

10 § *Varje myndighet eller enhet som har signalskyddsmateriel ska förteckna materielen i ett register. Av registret ska det framgå var materielen finns och*

dess individnummer. Registret ska ständigt hållas aktuellt.

Dokumentationen kan göras i ett av myndigheten utpekat system eller i ett separat dokument. Förteckningen ska så långt möjligt överensstämma med kvittenserna som gjordes vid utlämningen av signalskyddsmateriel.

11 § *Signalskyddsmateriel som finns inom svenskt territorium ska inventeras varje år och signalskyddsmateriel som finns utomlands ska inventeras var sjätte månad. Inventering av signalskyddsmateriel ska även göras vid byte av befattningshavare som ansvarar för sådan materiel.*

Signalskyddschefen ska se till att inventeringen utförs av en signalskyddsutbildad person.

Inventeringen ska dokumenteras och bevaras i minst 5 år.

Resultatet efter genomförd inventering ska kontrolleras mot enhetens register över signalskyddsmateriel. Brister som har framkommit i samband med en inventering ska utredas i syfte att klarlägga om det föreligger en materielincident eller inte. Utredningen ska dokumenteras.

Stöldrisken och underrättelsehotet bedöms som större utomlands varvid det finns ett särskilt krav vad gäller inventering av materiel utomlands. Det är viktigt att omständigheterna kring eventuella brister utreds så att de som tilldelat materielen kan ersätta förlusten samt att myndigheten kan vidta nödvändiga åtgärder så att brister i förvaring och uppföljning inte upprepas. Förlust eller manipulation av signalskyddsmateriel är en materielincident och ska rapporteras och omhändertas enligt reglerna för materielincident i 17 §. Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

Utlåning

12 § *En myndighet får låna ut signalskyddsmateriel till någon som omfattas av föreskrifterna i denna författning. I övriga fall måste skriftligt avtal ha ingåtts*

mellan myndigheten och den som mottar materielen om att tillämpa innehållet i denna författning.

Vid utlåning mellan myndigheter eller annan avtalad verksamhet krävs kvittering av materielen enligt 3 kap. 7 §. De företag som tilldelats signalskydd i någon form ska i ett avtal med en statlig myndighet förbinda sig att följa denna författning.

13 § *Signalskyddsmateriel får lånas ut till en utländsk myndighet eller en mellanfolklig organisation endast om det finns en giltig internationell signalskyddsöverenskommelse.*

En signalskyddsöverenskommelse får endast upprättas av myndigheter som är bemyndigade av regeringen. En signalskyddsöverenskommelse är giltig först efter att samtliga parter undertecknat överenskommelsen.

Överlåtelse

14 § *Signalskyddsmateriel får överlåtas endast till en annan statlig myndighet.*

Med överlåtas menas att signalskyddsmateriel byter ägare i Försvarsmaktens centrala materieluppföljningssystem.

Avveckling och förstöring

15 § *Vid avveckling av en enhets signalskyddsverksamhet eller när signalskyddsmateriel inte längre behövs ska materielen inventeras och återlämnas till den som tilldelat materielen. Inventeringen ska genomföras på det sätt som anges i 11 §.*

Normalt återlämnas materiel inom Försvarsmakten samt de försvarsmaktsnära myndigheterna till FCIS och för övriga myndigheter till FRA i Sollefteå.

16 § *Signalskyddsmateriel får endast förstöras med en metod som är godkänd av Högkvarteret.*

Det är skillnad på kontrollerad förstöring av materiel, som exempelvis sker i samband med ett beslut om att avveckla ett signalskyddssystem, och ett hastigt uppkommet behov av förstöring av materiel som kan behöva genomföras för att materielen inte ska falla i orätta händer. I det första fallet ska materielen sändas tillbaka till centralt förråd som för Försvarsmakten samt de försvarsmaktsnära myndigheterna normalt är FCIS. För övriga myndigheter innebär det normalt FRA i Sollefteå.

I det andra fallet gällande metoder för hastigt uppkommet behov av förstöring av signalskyddssystem finns dessa i förekommande fall definierade i signalskyddssystemets säkerhetsmässiga krav. Om tiden medger ska dock följande åtgärder vidtas:

1. Nödradering.
2. Kryptoapparaten förstörs så den blir obrukbar. Hur detta genomförs rent praktiskt avgörs av den specifika verksamhetens möjligheter.

Åtgärder vid materielincident

17 § *Den som har förlorat eller inte kan återfinna signalskyddsmateriel, eller misstänker manipulation av eller åverkan på signalskyddsmateriel eller dess försegling, ska omedelbart anmäla detta. Anmälan ska ske till myndighetens eller enhetens signalskyddschef, säkerhetsskyddschef och till den som tilldelat materielen samt till Högkvarteret.*

Finns misstanke om att manipulation eller åverkan har skett på signalskyddsmateriel eller dess försegling ska materielen omedelbart tas ur drift.

Tidigare krav på att signalskyddsmaterielen ska hanteras som hemlig är borttaget då materielen ska betraktas som skyddsvärd och alltid ska hanteras så att manipulation och tillgrepp förhindras. Om signalskyddsmateriel tas ur drift p.g.a. en incident ska den överlämnas till signalskyddschefen som ser till att materielen

omhändertas på ett korrekt sätt intill dess att den kan skickas till utpekad kryptoverkstad.
Om det vid incidenten fanns inlästa signalskyddsnycklar i kryptoapparaten ska även en anmälan om nyckelincident upprättas.
Inom Försvarsmakten är en incident med signalskyddsmateriel att betrakta som en säkerhetsincident och den ska även rapporteras som en säkerhetshändelse till regional stab eller Högkvarter. För övriga myndigheter gäller respektive myndighets säkerhetsbestämmelser.

4 kap. Aktiva kort

1 § *TAK och NBK får endast användas i kortterminaler eller kortläsare som har godkänts av Högkvarteret och endast tillsammans med programvaror som är godkända för TAK respektive NBK.*

För TAK och NBK är godkända kortläsare normalt KT2 eller KT ADM. TEID får användas i kommersiella kortläsare.

2 § *Till varje TAK och TEID ska kvitto för aktiva kort upprättas i två exemplar. Ett kvittoexemplar ska efter kvittens av kortanvändaren återsändas till Högkvarteret. Det andra kvittoexemplaret ska förvaras av användaren.*

Användaren ska upplysas om att hen ska förvara kvitton och datapost säkert och att dessa handlingar finns tillgängliga vid behov.

Utgivning och personalisering

3 § *En myndighet eller enhet som ska ge ut och knyta ett TAK och TEID till en viss person eller funktion (personalisering) får endast använda utrustning, programvara och metoder som har godkänts av Högkvarteret.*

I samband med personalisering får TAK och TEID endast hanteras i tillträdesbegränsat utrymme och så att obehöriga inte får insyn i verksamheten.

Aktiva kort ska förtecknas i ett register. Av registret ska framgå kortets serienummer, kortinnehavare samt i förekommande fall certifikat.

Stycke ett och två riktar sig endast till MUST SÄKT då TAK och TEID skapas/personaliseras. Stycke tre riktar sig till både MUST SÄKT samt de myndigheter som nyttjar TAK och/eller TEID. Kortregistret kan föras i ett av myndigheten utpekat system (exempelvis TSA-rutinen i IS UNDSÄK eller CertOrder) eller i ett separat dokument.

Förpackning och distribution

4 § *Varje myndighet ska se till att nödvändiga skyddsåtgärder vidtas vid distributon av aktiva kort.*

Aktiva kort ska distribueras i ett förseglat emballage. Emballaget ska vara så beskaffat att det inte går att ta del av innehållet utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget.

Det förseglade emballaget ska innehålla ett förseglat innerkuvert som ska vara försett med påskrift att det innehåller aktiva kort och att det ska överlämnas obrutet till den som är kortadministratör eller till den som myndigheten har bestämt.

Emballage kan vara kuvert förseglat med säkerhetstejp eller säkerhetspåse. Innerkuvertet syftar till att inte exponera nycklarna i onödan för exempelvis expeditionspersonal som tar emot försändelsen.

5 § *När aktiva kort distribueras ska ett mottagningsbevis och en följesedel samt i förekommande fall kvitton bifogas. Av följesedeln ska framgå kortens serienummer och vem de är avsedda för. Följesedeln ska registreras vid mottagandet och bevaras i minst 10 år. Mottagningsbeviset ska snarast undertecknas och återsändas till avsändaren.*

Vid mottagning av försändelse med aktiva kort ska innehållet i försändelsen

snarast efter mottagandet kontrolleras mot bifogad följesedel. Överensstämmer inte innehållet i försändelsen med bifogad följesedel ska anmälan om incident med aktiva kort omedelbart göras enligt vad som föreskrivs i 3 kap. 17 §.

Det är viktigt att mottagningsbeviset och följesedeln bipackas där de aktiva korten finns. Detta för att det är kortadministratören eller någon annan utsedd person som tar emot de aktiva korten som ska kontrollera att alla aktiva kort finns med enligt följesedeln samt därefter återsända mottagningsbeviset.

Det är för signalskyddstjänsten viktigt att innehållet kontrolleras skyndsamt så att eventuella misstag kan rättas till.

Försvarsmakten är numera en registratormyndighet vilket innebär att där en handling (exempelvis en följesedel) upprättas där ska handlingen också registreras. Handlingar som skickas och tas emot inom Försvarsmakten behöver mottagande enhet inte registrera då handlingen redan är registrerad av upprättande enheten. Är handlingen däremot att betrakta som inkommen från annan myndighet eller verksamhet ska den registreras där den inkom.

Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

Utlämning

6 § *När aktiva kort ska lämnas ut ska användarens identitet kontrolleras och kortet ska därefter kvitteras av mottagaren.*

Det tidigare kravet på att det endast var kortadministratören som fick lämna ut aktiva kort är borttaget för att skapa handlingsutrymme vid verksamheter som hanterar aktiva kort. Totalförsvarets signalskyddsskola, TSS, har tagit fram ett informationsunderlag som kortadministratören kan använda vid utbildning av personal som endast ska lämna ut och ta emot aktiva kort.

Inläsning av signalskyddsnycklar

7 § *Signalskyddsnycklar för samtliga signalskyddsgrader får läsas in i TAK och NBK enligt denna författning samt de säkerhetsmässiga kraven som Högkvarteret meddelar för signalskyddstjänsten. I ett TEID får endast signalskyddsnycklar för SG R och SG TRF läsas in.*

Signalskyddsnycklar för olika signalskyddsgrader får inte samtidigt vara inlästa i samma aktiva kort med undantag för signalskyddsnycklar för SG S och SG C som får vara inlästa i samma aktiva kort, och signalskyddsnycklar för SG R och SG TRF som får vara inlästa i samma aktiva kort.

Ett aktivt kort med inlästa signalskyddsnycklar för SG TS får inte samtidigt ha inlästa signalskyddsnycklar med andra signalskyddsgrader.

För aktivt kort som har haft inlästa signalskyddsnycklar upp till och med SG R eller SG TRF ska byte av kortets kod göras innan signalskyddsnycklar för SG TS eller SG S och SG C läses in.

Förvaringskraven för signalskyddsnycklar inläst på aktivt kort följer de förvaringskrav som gäller för signalskyddsnycklar. Aktiva kort med inlästa signalskyddsnycklar övertar nycklarnas klassning då de är inlästa i vilket innebär att de då måste stå under ständig uppsikt, vara under kontroll eller låsas in i ett säkerhetsskåp när det gäller signalskyddsnycklar märkta med SG C, SG S och SG TS. För signalskyddsnycklar märkta med SG R och SG TRF gäller ständig uppsikt, vara under kontroll alternativt inlåsta eller förvarade i en lokal som endast den som är behörig att ta del av nycklarna har tillträde till.

Byte av kod på aktiva kort som har haft inlästa signalskyddsnycklar upp till och med SG R eller SG TRF syftar till att minska intrångsrisken då det aktiva kortet har använts i signalskyddssystem med en lägre skyddsnivå.

Hantering och förvaring

8 § *Aktiva kort som innehåller signalskyddsnycklar ska hanteras och förvaras på samma sätt som föreskrivs om signalskyddsnycklar i 2 kap. 11–13 §§.*

En myndighet eller enhet ska vidta säkerhetsskyddsåtgärder i syfte att förhindra manipulation och tillgrepp av aktiva kort utan inlästa signalskyddsnycklar. Åtgärderna ska dokumenteras.

Åtgärderna kan med fördel dokumenteras i den ordinarie signalskyddsinstruktionen och kan innehålla krav på att exempelvis kontorsrum, där aktiva kort utan inlästa nycklar används, ska hållas låsta om ingen behörig personal finns i utrymmet. Vidare kan exempelvis ett krav vara att ett aktivt kort, utan inlästa nycklar, ska hanteras som användarens bankkort.

Datapost för TAK och NBK ska hållas under ständig uppsikt eller förvaras inlåst i säkerhetsskåp. Datapost för TEID ska skyddas mot manipulation och tillgrepp t.ex. genom ständig uppsikt, vara under kontroll eller förvaring i ett låst utrymme.

Åtgärder vid incident med aktivt kort

9 § *Den som har förlorat eller inte kan återfinna ett aktivt kort, misstänker eller på annat sätt har fått uppgift om att någon obehörig har haft tillgång till eller manipulerat ett aktivt kort, ska omedelbart anmäla detta. Anmälan ska ske till kortadministratör, myndighetens eller enhetens signalskyddschef och säkerhetsskyddschef samt till Högkvarteret.*

Det är för signalskyddstjänsten viktigt att en kortincident hanteras skyndsamt så att eventuella misstag kan rättas till. Om det vid incidenten fanns inlästa kryptonycklar på kortet ska även en anmälan om nyckelincident upprättas.

Inom Försvarsmakten är en incident med aktiva kort att betrakta som en säkerhetsincident och ska även rapporteras som en säkerhetshändelse till regional stab eller Högkvarter. För övriga myndigheter gäller respektive myndighets säkerhetsbestämmelser.

5 kap. Internationella signalskyddsöverenskommelser

1 § *En myndighet som förhandlar om att ingå en internationell signalskyddsöverenskommelse avseende svensk signalskyddsmateriel ska beakta föreskrifterna i denna författning. Endast om det föreligger särskilda skäl får myndigheten ingå en överenskommelse med lägre ställda krav på hantering och förvaring av signalskyddssystem än som framgår av denna författning.*

Detta får ske först efter överenskommelse med Högkvarteret.

När utländsk personal ska använda svenska signalskyddssystem ska de normalt använda och hantera systemet på samma sätt som svensk personal. Samma krav på behörighet och signalskyddsutbildning ska gälla.

2 § *Bestämmelserna i en internationell signalskyddsöverenskommelse avseende utländsk signalskyddsmateriel som ställer högre krav på hantering och förvaring av signalskyddssystem har företräde framför föreskrifterna i denna författning.*
I övrigt har föreskrifterna i denna författning företräde.

Vid hantering av utländska signalskyddssystem gäller som grund de svenska reglerna för signalskyddstjänsten. Det kan dock tillkomma ytterligare krav såsom att utländsk materiel inte får postförsändas utan endast får transporteras av utbildad personal. Utländska signalskyddssystem som tilldelats Sverige som slutanvändarland får i normalfallet aldrig lånas ut eller säljas till något annat land och inte heller exponeras för utländska medborgare.

6 kap. Undantag

1 § *Försvarsmakten får medge undantag från föreskrifterna i denna författning.*

Överbefälhavaren, eller den Överbefälhavaren bestämmer, fattar beslut i ärenden om undantag.

Överbefälhavaren har inte bestämt att någon annan än Överbefälhavaren får fatta beslut i ärenden om undantag.

Denna författning träder i kraft den 1 februari 2017.

Genom författningen upphävs Försvarsmaktens föreskrifter (FFS 2005:2) om signalskyddstjänsten inom totalförsvaret.

Micael Bydén

Carin Bratt

Bilaga 1 Signalskyddsgrader

Ett signalskyddssystem ska i samband med Högkvarterets godkännande placeras i någon av nedan angivna signalskyddsgrader med följande beteckningar och betydelser.

Beteckning	***Betydelse***
Signalskyddsgrad Top Secret (SG TS)	*Signalskyddssystemet är godkänt för att skydda information som* *1. är av synnerlig betydelse för rikets säkerhet (kvalificerat hemlig),* *2. är placerad i informationssäkerhetsklassen HEMLIG/TOP SECRET,* *3. har åsatts beteckningen TOP SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation, eller* *4. om den röjs skulle förorsaka totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation synnerligt men.*
Signalskyddsgrad Secret (SG S)	*Signalskyddssystemet är godkänt för att skydda information som* *1. är hemlig,* *2. är placerad i informationssäkerhetsklassen HEMLIG/SECRET,* *3. har åsatts beteckningen SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation, eller* *4. om den röjs skulle förorsaka totalförsvaret eller*

	förhållandet till en annan stat eller en mellanfolklig organisation betydande, men inte synnerligt, men.
Signalskyddsgrad Confidential (SG C)	*Signalskyddssystemet är godkänt för att skydda information som* 1. *är hemlig,* 2. *är placerad i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL,* 3. *har åsatts beteckningen CONFIDENTIAL eller motsvarande av en utländsk myndighet eller mellanfolklig organisation, eller* 4. *om den röjs skulle förorsaka totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation inte obetydligt, men inte betydande eller synnerligt, men.*
Signalskyddsgrad Restricted (SG R)	*Signalskyddssystemet är godkänt för att skydda information som* 1. *är hemlig,* 2. *är placerad i informationssäkerhetsklassen HEMLIG/RESTRICTED,* 3. *har åsatts beteckningen RESTRICTED eller motsvarande av en utländsk myndighet eller mellanfolklig organisation, eller* 4. *om den röjs skulle förorsaka totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation endast ringa men.*
Signalskyddsgrad Trafikskydd (SG TRF)	*Signalskyddssystemet är godkänt för skydd av telekommunikation mot obehörig insyn i och påverkan av telekommunikations- och IT-system.*

Ett sådant signalskyddssystem (SG TRF) är dock inte godkänt för skydd av hemliga uppgifter.

Bilaga 2 Signalskyddsinstruktion

Enligt 1 kap. 9 § i denna författning ska signalskyddsinstruktionen innehålla uppgifter om

1. myndighetens eller enhetens signalskyddsorganisation,

2. åtgärder vid

- krishantering och höjd beredskap,

- signalskyddsincident,

3. enhetens signalskyddsutbildade personal, dess behörigheter och, i förekommande fall, placering i signalskyddsbefattning,

4. enhetens tilldelade signalskyddsnycklar samt var dessa förvaras,

5. rutiner för beställning, mottagning, extern och intern distribution, delgivning, kvittens, förvaring, inventering och förstöring av signalskyddsnycklar samt, i förekommande fall, lokal produktion av signalskyddsnycklar,

6. enhetens tilldelade signalskyddsmateriel samt var den är placerad och förvarad,

7. rutiner för beställning, mottagning, extern och intern försändning, utlämning, kvittens, förvaring, inventering, reparation och återlämning av signalskyddsmateriel,

8. enhetens register över aktiva kort, och

9. rutiner för beställning, mottagning, extern och intern försändning, utlämning, förvaring och återsändning av aktiva kort.

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.